H2554 PCT

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2002 (12.09.2002)

PCT

(10) International Publication Number
WO 02/071238 A1

(51) International Patent Classification[7]: G06F 13/00

(21) International Application Number: PCT/US02/06775

(22) International Filing Date: 6 March 2002 (06.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/273,847 6 March 2001 (06.03.2001) US

(71) Applicant *(for all designated States except US)*: **E-MOOLA, INC.** [US/US]; 129 W. Wilson Street, Suite 105, Costa Mesa, CA 92627 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MORGAN, Russell** [AU/US]; 2917 Silver Lane, Newport Beach, CA 92660 (US). **HEMSLEY, Adam** [AU/US]; 84 Lyon Street, Amsterdam, NY 12010 (US).

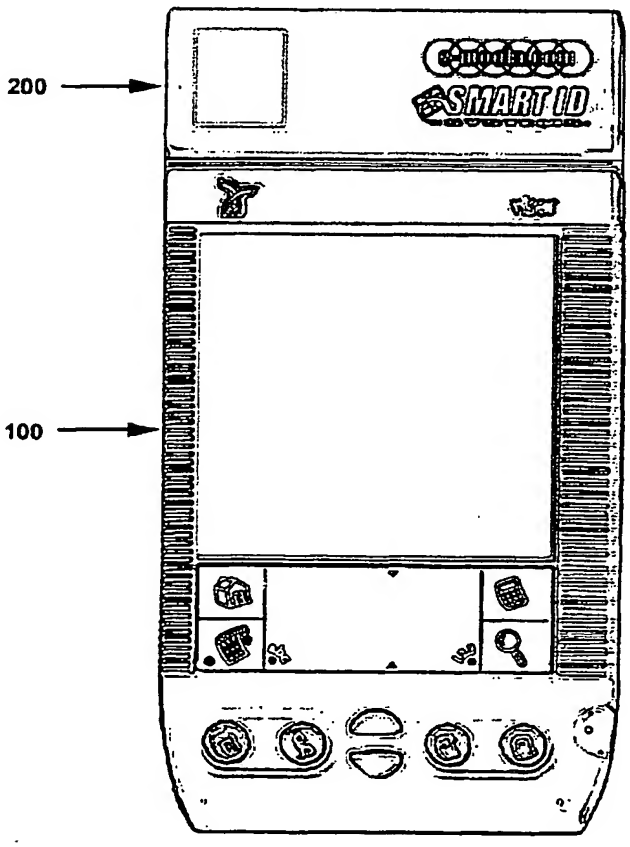
(74) Agents: **HOKANSON, Jon, E.** et al.; Small Larkin, LLP, 18th Floor, 10940 Wilshire Boulevard, Los Angeles, CA 90024 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: SECURE SMART-ID PALMTOP DOCKING MODULE



(57) Abstract: The present invention describes an expansion module for a handheld computer which allows the handheld computer (100) and expansion module (200) to function together as a secure security-ID terminal that accepts IC based ID-cards (Smart Card) and IC based "dog-tags" and presents the information to security personnel to validate the card holders authority to enter into a secure area. The present invention utilizes photo-ID and biometric data stored on the IC based ID-card (Smart Card) and IC based "dog-tag" to validate that the person presenting the credentials is in fact the person authorized to be presenting them. The resultant mobile secure security-ID terminal meets the advanced security requirements of military and non-military security sites worldwide. By disconnecting the handheld computer from the expansion module, the handheld computer is restored to conventional operation.

WO 02/071238 A1

European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SECURE SMART-ID PALMTOP DOCKING MODULE.

TECHNICAL FIELD

There is a need for a truly portable secure security ID system. The present invention converts a standard handheld computer into a secure security-ID terminal by utilizing a special expansion module and the 'plug-and-play' functionality of the expansion slot provided on some handheld computers. The present invention includes mechanical structures enabling entry of IC based ID-card (Smart Card) information via either contact or contactless methods. The present invention also incorporates a thumbprint scanner to further improve the security and accuracy of the device.

This new entity of the handheld computer and expansion module then becomes the secure security-ID terminal that accepts input from IC based ID-card (Smart Card) or IC based 'dog-tags'.

BACKGROUND ART

U.S. Pat. No. 5,465,038 to Register (Register) discloses a battery charging/data transfer apparatus for a handheld computer, the battery charging/data transfer structure is provided for use in conjunction with a handheld computer to charge its battery and serve as an infrared data exchange interface between the handheld computer and a data input/output device such as a desktop computer.

U.S. Pat. No. 5,157,769 to Eppley (Eppley) discloses a computer data interface for connecting a handheld computer and a desktop computer. The computer data interface includes a cable having connectors at each end thereof. Mounted in one of the connectors is an adapter circuit for receiving data signals from the handheld computer and transmitting the signals to the desktop computer at a voltage levels compatible with the desktop computer. Similarly, the adapter circuit receives signals from the desktop computer and transmits the signals to the handheld computer at voltage levels compatible with the handheld computer. The adapter circuit is powered by the desktop computer to prevent draining the batteries of the handheld computer.

U.S. Pat. No. 5,878,276 to Aebli (Aebli) discloses a computer system, and particularly a handheld mobile client system, in which a user input device such as a keyboard or a scanner, coupled by a tethering conductor or a wireless link such as an infrared radiation link, functions as a master while the central processing unit of the system functions as a slave in receiving input digital signals.

U.S. Pat. No. 6,115,248 to Canova (Canova) discloses a detachable securement of an accessory device to a handheld computer, that provides for coupling an accessory device to a back face of a handheld computer while electrically connecting to the handheld computer through a communications or output port. In one embodiment, the accessory device "piggy-backs" on the handheld computer so that the accessory device and handheld computer form a portable combination. An insertion coupling may be used to detachably secure the accessory device with the handheld computer. The insertion coupling used with embodiments of the invention is preferably a snap-in coupling having one or more biased members. The biased members may be contracted to engage an aperture on a back face of the handled computer. When released, the biased members secure the accessory device to the handheld computer.

U.S. Pat. No. 6,144,848 to Walsh (Walsh) discloses a handheld remote computer control and methods for secured interactive real-time telecommunications, that describes an interactive bi-directional telecommunication method using a handheld low power user device to access a host computer server along a telecommunication path, and to command the host computer server to transmit audio and/or visual reports to the user device. A system for host computer ordering of consumer products and services using the telecommunications method and handheld low power user device.

U.S. Pat. No. 5,974,238 to Chase, Jr., (Chase) discloses an automatic data synchronization between a handheld and a host computer using pseudo cache including tags and logical data elements, that describes an apparatus for performing dynamic synchronization between data stored in a handheld computer and a host computer, each having a plurality of data sets including at least one

common data set, each computer having a copy of the common data set. The handheld computer has a processor, a communication port, and a data synchronization engine. The data synchronization engine has a pseudo-cache and one or more tags connected to the pseudo cache. Data is synchronized whenever data is written to main memory and/or when the associated pseudo-cache tag is invalidated. By strict adherence to a set of protocols, data coherency is achieved because the system always knows who owns the data, who has a copy of the data, and who has modified the data. The data synchronization engine resolves any differences in the copies and allows the storage of identical copies of the common data set in the host computer and in the handheld computer.

DISCLOSURE OF INVENTION

It is an object of this invention to provide an improved vehicle for the acceptance of security ID information from IC based ID-card (Smart Card) or IC based 'dog-tags' as found in military ID applications or high security requirements and other areas where accurate security ID is required.

In application, the security guard either inserts the IC based ID-card (Smart Card) into the ID Card reader of the expansion module, or the security guard places the secure security-ID terminal in close proximity of the IC based ID-card (Smart Card) or IC based 'dog-tag' so that the information contained therein can be read utilizing conventional contactless methods of reading information from contactless ID Card products. It will be understood that as used herein, the term "security guard" refers to any person operating the present invention as disclosed herein.

The microprocessor on the handheld computer reads the security ID information from the IC based ID-card (Smart Card) or IC based 'dog-tag.' The validity of the data contained in the IC based ID-card (Smart Card) or IC based 'dog-tag' is checked by displaying the Name, Rank and Photo of the authorized user of the IC based ID-card (Smart Card) or IC based 'dog-tag' on the display of the handheld computer for visual comparison by the security guard. The

microprocessor on the handheld computer also compares the security ID information from the IC based ID-card (Smart Card) or IC based 'dog-tag' against a database of authorized individuals contained within the expansion module, and any discrepancy may be highlighted on the screen of the handheld computer. The microprocessor on the handheld computer may additionally request a thumb-print scan of the holder of the IC based ID-card (Smart Card) or IC based 'dog-tag' in high security areas as further validation that it is the authorized user who is proffering the IC based ID-card (Smart Card) or IC based 'dog-tag'.

If the microprocessor on the handheld computer determines that the thumbprint proffered does not match the thumbprint signature from the IC based ID-card (Smart Card) or IC based 'dog-tag', the thumbprint is then deemed to be not valid, and the microprocessor on the handheld computer displays an appropriate message on the handheld computer's screen that access should be denied and other appropriate action initiated.

If the microprocessor on the handheld computer determines that the proffered IC based ID-card (Smart Card) or IC based 'dog-tag' does not match a corresponding entry in the authorized individual database contained within the expansion module, then the IC based ID-card (Smart Card) or IC based 'dog tag' is deemed to be not valid, and the microprocessor on the handheld computer displays an appropriate message on the handheld computer's screen that access should be denied and other appropriate action initiated.

The microprocessor on the handheld computer records the details of every IC based ID-card (Smart Card) or IC based 'dog-tag' read in another database in the expansion module. This database is then accessed when the handheld computer is placed within the charging docking module to update the main site database of access authorizations and denials. This is also the time when the main site database would update the authorized personnel database contained within the expansion module in a similar manner.

BRIEF DESCRIPTION OF THE DRAWINGS

Detailed drawings of the present invention are shown in the attached Figures, in which:

FIGURE 1 shows a front view of an electrically connected handheld computer and expansion module according to the present invention;

FIGURE 2 shows a diagram of the major components of an electrically connected handheld computer and expansion module and their interconnection, according to the present invention;

FIGURE 3 shows a flow diagram of the actions and responses involved during the process of a typical transaction;

FIGURE 4 shows a diagrammatic illustration of representative types of IC based ID-card (Smart Card) and IC based 'dog-tag' accepted by the present invention;

FIGURE 5a shows a top view of the handheld computer and the expansion module connector;

FIGURE 5b shows a top view of the expansion module;

FIGURE 6 shows a front view of the coupled handheld computer and expansion module according to the present invention;

FIGURE 7 shows a side view of the coupled handheld computer and expansion module according to the present invention; and

FIGURE 8 shows the function of the signals typically found on the pins of the auxiliary connector of a conventional Handspring handheld computer.

BEST MODE FOR CARRYING OUT THE INVENTION

The present invention is a coupled handheld computer expansion module system that provides a secure security identification (security-ID) terminal for high security access applications.

Figure 1 is a diagrammatic illustration of a preferred embodiment of the system that includes a conventional handheld computer 100, along with an expansion module 200, that together form a secure security-ID terminal of the present invention. In one preferred embodiment, a Handspring Visor Prism brand handheld computer 100 is utilized and uses a connection via the handheld computer expansion connector 106 (not shown) and expansion module mating connector 201 (not shown). The Handspring Visor Prism handheld computers are manufactured by Handspring, an American manufacturer of handheld computers and a leading supplier to the world market. There are handheld computers made by other manufacturers that conform to the Springboard Expansion Module standard that may be used with the present invention.

Figure 2 schematically illustrates a typical handheld computer 100 as mated to the expansion module 200 to form the secure security-ID terminal of the invention. Customarily, Handspring Visor Prism handheld computers have a colour display 101, keypad 102 and touchpad 103 that are electronically connected to each other via a bus structure 105 that also interfaces with a conventional microprocessor 104. The microprocessor 104 typically used in Handspring Visor Prism handheld computers is the MC68VZ328 Dragonball-VZ microprocessor manufactured by Motorola. The above described hardware configuration is powered by replaceable batteries 107 and this is a common configuration in most handheld computers.

Handspring has established a particular protocol for interfacing between the microprocessor 104 and expansion module 200. This interface allows the facilities of the expansion module to be accessed from the handheld computer 100 via the

handheld computer expansion connector 106. This interface allows addition programs, memory and other devices to be made available to and be controlled by the handheld computer's microprocessor 104. Information about the interface can be found in the Springboard Development Guide for Handspring Handheld Computers (Document No. 80-0091-00) and the Handspring Development Tools Guide (Document No. 80-0092-00) obtainable from the www.handspring.com website.

The interface protocol, hardware and system described above are believed to be equivalent in all handheld computers that conform to the Springboard standard. Accordingly, the present invention is not limited to use with Handspring handheld computers, or limited to brand specific Handspring handheld computer models.

The handheld computer expansion connector 106 typically contains 70 contacts (Figure 8), including 16-data lines, 24-address lines, control signals, power and ground. All of these signals are with reference to the handheld computer. These signals mate with the matching connector 201 on the expansion module 200. Full details of the pin definitions, signal specifications and timing parameters are published in the Handspring Product Guide: Visor Prism (Document No. 80-0094-00) that may also be obtained from the www.handspring.com website.

The handheld computer 100 communicates with the expansion module 200 by accessing the expansion module 200 through the handheld computer expansion connector 106, to the expansion module control assembly 202, via the mating connector 201 as detailed in the SpringBoard specifications. Additional embodiments may also contain a microprocessor 203 on the expansion module control assembly 202 to perform additional processing or security related functions.

A preferred microprocessor for use as the expansion module microprocessor 203 of the present invention is a Motorola MC68HC711. Other microprocessors adapted to control the functioning of the expansion module 200 may be used in the present invention and are functionally equivalent.

The expansion module control assembly 202 contains a smart card proximity reader 209 and also contains an ID Card reader 205 that mates with, and accepts data from IC cards or, as they are commonly known, "Smart Cards." The expansion module control assembly 202 also includes a thumbprint scanner 210 and a conventional Multifunction Secure Access Module (SAM) 204. The Multifunction Secure Access Module (SAM) 204 is a sub-assembly that contains a special microprocessor, memory and encryption processor, encapsulated as a SIM module, similar to the conventional SIM modules found in modern mobile phones, that is used to securely perform all the required cryptographic functions as described herein. The expansion module control assembly 202 also contains an internal battery 207 that is recharged whenever the handheld computer is plugged into it's conventional docking module (not shown). This internal battery 207 is used to power the features found on the expansion module, and to provide data retention when the expansion module is not in use.

Figure 3 is a diagrammatic flowchart illustrating preferred operational steps and information flow for the present invention. When security personnel read the information from an IC based 'dog-tag' 401 through the expansion module's smart card proximity reader 209, the reader detects the 'dog-tag' information at step 300, the microprocessor 104 then performs a cryptographic validation and expiration check on the account number read from the IC based 'dog-tag' 401 at step 302 and 303 utilising the Multifunction Secure Access Module (SAM) 204. The micro processor 104 uses conventional cryptographic validation routines as provided in the relevant ISO standards, such as ISO Standard 15408. The microprocessor 104 determines whether it should authenticate the 'dog-tag' offline using either offline static or dynamic data authentication based upon the 'dog-tag' and terminal support for these methods.

Offline Static Data Authentication (SDA) validates that important application data has not been fraudulently altered since 'dog-tag' personalization. The terminal validates static (unchanging) data from the 'dog-tag' using the 'dog-tag's' Issuer Public Key (PK) Certificate that contains the Issuer Public Key and a digital signature that contains a hash of important application data encrypted with the

Issuer Private Key. The terminal recovers the Issuer Public Key from the Issuer PK Certificate and uses the recovered Issuer Public Key to recover the hash of application data from the digital signature. A match of the recovered hash with a hash of the actual application data proves that the data has not been altered.

Offline Dynamic Data Authentication (DDA) validates that the 'dog-tag' data has not been fraudulently altered and that the 'dog-tag' is genuine. The terminal verifies the 'dog-tag' static data in a similar manner to SDA. Then, the terminal requests that the 'dog-tag' generate a cryptogram using dynamic (transaction unique) data from the 'dog-tag' and terminal and an ICC Private Key. The terminal decrypts this dynamic signature using the ICC Public Key recovered from 'dog-tag' data. A match of the recovered data to the original data verifies that the 'dog-tag' is not a counterfeit 'dog-tag' created with data skimmed (copied) from a legitimate 'dog-tag'.

Alternatively, when the security personnel inserts a IC based ID-card (Smart Card) 400 into the ID Card reader slot 208, the microprocessor 104 detects the IC based ID-card (Smart Card) 400 insertion into the ID Card reader 205 at step 301, and microprocessor 104 performs a cryptographic validation and expiration check on the account number read from the IC based ID-card (Smart Card) 400 at step 302 and 303 utilizing the SAM 204. The microprocessor 104 uses conventional cryptographic validation routines as provided in the relevant ISO standards, such as ISO Standard 15408. The microprocessor 104 determines whether it should authenticate the card offline using either offline static or dynamic data authentication based upon the card and terminal support for these methods.

Offline Static Data Authentication (SDA) validates that important application data has not been fraudulently altered since card personalization as discussed above in regard to the IC based 'dog-tag.'

If the microprocessor 104 determines that the account number is not valid at step 303, an "Invalid ID Card" message or other appropriate message is displayed on the handheld computer's display 101 at step 304. The microprocessor 104 will then update the site access record to show that this ID has not been validated for

site access at step 305. In a typical security scenario – the security guard will deny access and take whatever action is appropriate for the circumstances, (e.g. keep the ID badge – call authorities) at step 306.

If the microprocessor 104 determines that the offered ID card is valid, the handheld computer's microprocessor 104 checks the cardholders authorization to enter the secure area against a database held within the handheld computer's memory at step 307.

If an authorization for entry for the person submitting the ID badge cannot be found within the database within the handheld computer's memory at step 308, a "Request Orders" message is displayed on the handheld computer's display 101 at step 309. In appropriate circumstances the security guard will request any written orders or authorization for this ID card holder to enter this secure area at step 310. The security guard may then validate this written authorization using appropriate procedures at step 311 and 312. If the written authorization is not validated at step 312, the site record will be updated and the security guard will deny access at steps 305 and 306 as described previously.

If the written authorization is validated at step 312, the security guard will enter a temporary authorization code at step 313, and return the written orders to the ID card holder at step 314.

The microprocessor 104 will then update the site access record to show that the ID card identified in step 308 or 312 has been validated for site access.

The microprocessor 104 will then display the ID card holder's descriptive data on the handheld computer's display 101 at step 316, so that the security guard may perform a visual check between the information presented on the handheld computer's display 101 and the person presenting the ID card.

If the visual inspection does not match at step 318 – the site record will be updated and the security guard will deny access at steps 305 and 306 as described previously.

If the visual inspection at step 318 passes – the security guard will indicate that the visual inspection was OK at step 318, and the microprocessor 104 will update the site access record at 319 to show that this ID card visual identification in step 318 has been validated.

The microprocessor 104 will then determine if the site access requires thumbscan authorization at step 320. If thumbscan authorization is required by step 320, the microprocessor 104 will then display an "Obtain Thumbscan" message on the handheld computer's display 101 at step 321. The security guard will then obtain a thumbscan of the person presenting the ID card at step 322.

The microprocessor 104 using appropriate computer programming software contained within the expansion module 200 will then determine at step 323, if the thumbscan just obtained matches the thumbscan image data contained within the data read from the ID card at steps 300 or 301. If the thumbscan data does not match, the microprocessor 104 will display a "Thumbscan Fail" message on the handheld computer's display 101 at step 332, and the site record will be updated and the security guard will deny access at steps 305 and 306 as described previously.

If the thumbscan is validated at step 323, the microprocessor 104 will then update at 324 the site access record to show that this ID card thumbscan identification in step 323 has been validated.

If the thumbscan was not required at step 320, or the thumbscan data was validated at step 323, the microprocessor 104 will display an "Access Authorized" message on the handheld computer's display 101 at step 325 to advise the security guard that access has been authorized.

The security guard will acknowledge the "Authorized' message at step 326, the microprocessor 104 will then update the site access record to show that this ID card has been "Authorized" for access to this site at step 327.

At any time the handheld computer identifies that it has been placed into its standard power docking module at step 328, the site records will synchronize with

the information contained within the handheld computer and the site records will be updated at step 329.

Figure 4 diagrammatically illustrates the various types of cards accepted by the secure security-ID terminal of the present invention. The card types accepted are: - IC based ID-card (Smart Card)s 400, or IC based 'dog-tag' 401 that comprise of a base plastic card, a imbedded IC chip 402, and other printed and embossed information that is pertinent to the card (not shown). The IC based ID-card (Smart Card)s 400 and IC based 'dog-tags' 401 described herein conform in general to ISO 7810, ISO 7813, ISO 7816, ISO 10202 and ISO 14443.

Figure 5a is a diagrammatic illustration of a top view of a first preferred embodiment of the invention. It shows the handheld computer 100 and the location of the handheld computer expansion connector 106 on the top of the handheld computer 100.

Figure 5b is a diagrammatic illustration of a top view of the first preferred embodiment of the invention. It shows the expansion module 200 along with the location of the ID Card reader slot 208 location on top of the expansion module 200.

Figure 6 is a diagrammatic illustration of a front view of a first preferred embodiment of the invention. It shows the handheld computer 100 and expansion module 200 along with location details for the handheld computer's display 101, keypad 102 and touchpad 103. It also illustrates the preferred location of the thumbprint scanner 210.

Figure 7 is a diagrammatic illustration of a side view of a first preferred embodiment of the invention. It shows the handheld computer 100 and expansion module 200 along with location details for the handheld computer's display 101 (not seen), keypad 102 and touchpad 103 (not seen).

Figure 8 is a diagrammatic representation of the contact and signal configuration of a typical handheld computer. It shows the normal signals encountered on such a handheld computer.

In operation, the handheld computer 100 is electrically connected to the expansion module control assembly 202 via the handheld computer expansion connector 106. The handheld computer 100 includes, as is customary with most handheld computer's, a keypad 102, a touchpad 103 a display 101, memory (not shown) and a microprocessor 104. The handheld computer 100 is physically removably coupled to the expansion module 200.

In this invention, the microprocessor 104 continually monitors the activity of the expansion module's smart card proximity reader 209 and the ID Card reader 205 and continually monitors the activity within the handheld computer 100, and can capture information of each key press on the keypad 102, or touchpad 103 for processing under the control of the programs contained in the expansion module 200.

All handheld computer keypads 102 and touchpads 103 operate in a similar manner to control the functioning of the handheld computer 100. The handheld computer responds to key-presses on the keypads 102 and information stenciled on the touchpad 103 by the stylus, that are given in reply to prompts provided on the screen 101 by the program running in the handheld computer.

A conventional handheld computer 100 for use in the present invention, preferably includes a colour display 101, keypad 102 and touchpad 103 that are electronically connected via a bus 105 to microprocessor 104. This conventional handheld computer 100 will also customarily be provided with a powered docking module (not shown) that will provide battery recharge facilities, along with facilities to enable the data contained within the conventional handheld computer 100 to synchronize with an external database or source (not shown).

A preferred embodiment according to the present invention is one in which an IC based ID-card (Smart Card) 400 is used during the access authorization sequence. This preferred embodiment is described in detail below with reference to the accompanying drawings.

The security guard inserts the IC based ID-card (Smart Card) 400 through the IC based ID-card (Smart Card) slot 208 in the expansion module 200, the action of

inserting the IC based ID-card (Smart Card) 400 through the IC based ID-card (Smart Card) slot 208 in the expansion module 200 causes the stored information contained in the IC based ID-card (Smart Card) 400 to be read by the ID Card reader 205 and associated electronics on the expansion module control assembly 202 in such a manner as to present to the handheld computer microprocessor 104 the information contained in the IC of the IC based ID-card (Smart Card) 400.

The microprocessor 104 then performs a cryptographic validation and expiration check on the information read from the IC based ID-card (Smart Card) 400. The processor 104 uses conventional cryptographic validation routines as provided in the relevant ISO standards, such as ISO Standard 15408. The processor 104 determines whether it should authenticate the card offline using either offline static or dynamic data authentication based upon the card and terminal support for these methods.

Offline Static Data Authentication (SDA) validates that important application data has not been fraudulently altered since card personalization. The terminal validates static (unchanging) data from the card using the card's Issuer Public Key (PK) Certificate that contains the Issuer Public Key and a digital signature that contains a hash of important application data encrypted with the Issuer Private Key. The terminal recovers the Issuer Public Key from the Issuer PK Certificate and uses the recovered Issuer Public Key to recover the hash of application data from the digital signature. A match of the recovered hash with a hash of the actual application data proves that the data has not been altered.

Offline Dynamic Data Authentication (DDA) validates that the card data has not been fraudulently altered and that the card is genuine. The terminal verifies the card static data in a similar manner to SDA. Then, the terminal requests that the card generate a cryptogram using dynamic (transaction unique) data from the card and terminal and an ICC Private Key. The terminal decrypts this dynamic signature using the ICC Public Key recovered from card data. A match of the recovered data to the original data verifies that the card is not a counterfeit card created with data skimmed (copied) from a legitimate card.

If the proffered IC based ID-card (Smart Card) 400 is deemed to be not valid, an "Invalid ID Card" message or other appropriate message is displayed upon the display 101, and the site access record database (not shown) is updated by the microprocessor 104 to reflect the invalid ID card access attempt, and the security guard may take whatever action is appropriate for the circumstances.

If the proffered IC based ID-card (Smart Card) 400 is deemed to be valid – the card data is checked against a valid site access database (not shown) to determine if the proffered card has been authorized for access to this site. If the proffered card information is not found within the site access database (not shown), then the microprocessor 104 will display a "Request Orders" message on the display 101 for the security guard.

The security guard will then request the person proffering the IC based ID-card (Smart Card) 400 to present any written orders or authorization that authorize their access to this site. The security guard will validate the proffered orders or authorization using whatever procedure is required by the site in question. If the security guard is advised that the proffered documents are not valid, he will press a key on the keypad 102 to indicate to the program that the proffered documentation was found to be invalid, and the microprocessor 104 will display a "Invalid Orders" message on the display 101 and the site access record database (not shown) is updated by the microprocessor 104 to reflect the invalid orders access attempt, and the security guard will take whatever action is appropriate for the circumstances.

If the proffered documentation is found to be in order – the security guard will enter the temporary authorization number using the stylus on the touchpad 103, and return the proffered documentation to the person who presented the documentation. The site access record database (not shown) is updated by the microprocessor 104 to reflect the temporary authorization of this IC based ID-card (Smart Card) 400.

The microprocessor 104 will now display the information recovered from the proffered IC based ID-card (Smart Card) 400 for the security guard to view. This

information will include a photo-ID of the person authorized to use this IC based ID-card (Smart Card) 400 as well as such other data as required by site security.

The security guard will now perform a visual comparison of the information displayed on the display 101 and the person who proffered the card. If the security guard determines that there is not a match between the information displayed on the display 101 and the person who has proffered the card, he will press a key on the keypad 102 to indicate to the program that the visual match was found to be invalid. The microprocessor 104 will display a "Visual Match Fail" message on the display 101 and the site access record database (not shown) is updated by the microprocessor 104 to reflect the visual match failed, and the security guard will take whatever action is appropriate for the circumstances.

If the security guard determine that there is a match between the information displayed on the display 101 and the person who has proffered the card, he will press a key on the keypad 102 to indicate to the program that the visual comparison was found to be valid, and the site access record database (not shown) is updated by the microprocessor 104 to reflect the acceptance by the security guard of the visual check.

The microprocessor 104 would then check the site access database (not shown) to determine if additional biometric authorization is required for access to the site, by the person proffering the IC based ID-card (Smart Card) 400. If the microprocessor 104 determines that additional biometric authorization is required for the person proffering the IC based ID-card (Smart Card) 400, then the microprocessor 104 will display an "Obtain Thumbscan" message on the display 101, and the security guard will request a thumbscan from the person proffering the IC based ID-card (Smart Card) 400.

The microprocessor 104 will perform a validation of the thumbscan read by the thumbprint scanner 210 and compare it with the biometric data read from the IC based ID-card (Smart Card) 400 to determine if a sufficient match has been achieved to authorize access to the site. If the microprocessor 104 determines that the proffered thumbprint was not a sufficient match, then the microprocessor 104

will display a "Thumbscan Fail" message on the display 101 and the site access record database (not shown) is updated by the microprocessor 104 to reflect the failed thumbscan, and the security guard will take whatever action is appropriate for the circumstances.

If the microprocessor 104 determines that the proffered thumbprint is a sufficient match by predetermined criteria then the microprocessor 104 will update the site access record database (not shown) to reflect the accepted thumbscan.

The thumbscan (or scan of other body parts such as a finger, or the eye) validation is performed by conventional programs that use biometric authentication systems. The preferred validation program is eCryp FGP 1.0, available from and proprietary to eCryp, Inc., www.ecrypinc.com.

The microprocessor 104 will display an "Authorized" message on the display 101 and the site access record database (not shown) is updated by the microprocessor 104 to reflect that the person proffering the IC based ID-card (Smart Card) 400 has been cleared for access to the site. The security guard will press a key on the keypad 102 to indicate to the program to acknowledge the authorized message, and the microprocessor 104 will update the site access record database (not shown) to reflect the acceptance of the authorization.

Whenever the handheld computer 100 recognizes that it has been placed within it's docking module (not shown), as is conventional, the microprocessor 104 will synchronize it's databases (not shown) with the site main database (not shown), to reflect any changes or accesses granted or denied since the last time it synchronized with the site database in a manner similar to that disclosed in U.S. Pat. No. 5,974,238. At this time also any changes made to the site database are recorded in the database contained within the expansion module 200.

In a second embodiment according to the present invention an IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400 is used during the access authorization sequence. This embodiment is described in detail below with reference to the accompanying drawings.

The security guard places the expansion module 200 in the vicinity of the IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400 and presses a button on the keypad 102, the action of pressing the button on the keypad 102 causes the electronics contained within the expansion module 200 to inductively read the information stored in the IC based 'dog-tag' 401 or in a contactless IC based ID-card (Smart Card) 400, to be read by the smart card proximity reader 209 and associated electronics on the expansion module control assembly 202 in such a manner as to present to the handheld computer microprocessor 104 the information contained in the IC of the IC based 'dog-tag' 401 or of a contactless IC based ID-card (Smart Card) 400.

The microprocessor 104 then performs a cryptographic validation and expiration check on the information read from the IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400. The processor 104 uses conventional cryptographic validation routines as provided in the relevant ISO standards, such as ISO Standard 15408. The processor 104 determines whether it should authenticate the IC based 'dog-tag' or smart card offline using either offline static or dynamic data authentication based upon the IC based 'dog-tag' or smart card and terminal support for these methods.

If the proffered IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400 is deemed to be not valid, an "Invalid ID Card" message or other appropriate message is displayed upon the display 101, and the site access record database (not shown) is updated by the microprocessor 104 to reflect the invalid ID card access attempt. The security guard will then take whatever action is appropriate for the circumstances.

If the proffered IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400 is deemed to be valid – it is checked against a valid site access database (not shown) to determine if the proffered card or 'dog-tag' has been authorized for access to this site. If the proffered card or 'dog-tag' information is not found within the site access database (not shown), then the microprocessor 104 will display a "Request Orders" message on the display 101 for the security guard.

The security guard will then request the person proffering the IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400 to present any written orders or authorization that authorize their access to this site. The security guard will validate the proffered orders or authorization using whatever procedure is required by the site in question. If the security guard is advised that the proffered documents are not valid, he will press a key on the keypad 102 to indicate to the program that the proffered documentation was found to be invalid, and the microprocessor 104 will display a "Invalid Orders" message on the display 101 and the site access record database (not shown) is updated by the microprocessor 104 to reflect the invalid orders access attempt, and the security guard will then take whatever action is appropriate for the circumstances.

If the proffered documentation is found to be in order – the security guard will enter the temporary authorization number using the stylus on the touchpad 103, and return the proffered documentation back to the person who presented the documentation. The site access record database (not shown) is updated by the microprocessor 104 to reflect the temporary authorization of this IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400.

The microprocessor 104 will now display the information recovered from the proffered IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400 for the security guard to view. This information will include a photo-ID of the person authorized to use this IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400 as well as such other data as required by site security.

The security guard will now perform a visual comparison of the information displayed on the display 101 and the person who proffered the card. If the security guard determines that there is no match between the information displayed on the display 101 and the person who has proffered the card, he will press a key on the keypad 102 to indicate to the program that the visual match was found to be invalid. The microprocessor 104 will display a "Visual Match Fail" message on the display 101 and the site access record database (not shown) is updated by the

microprocessor 104 to reflect the visual match failed, and the security guard will take whatever action is appropriate for the circumstances.

If the security guard determines that there is a match between the information displayed on the display 101 and the person who has proffered the card or 'dog-tag,' he will press a key on the keypad 102 to indicate to the program that the visual comparison was found to be valid, and the site access record database (not shown) is updated by the microprocessor 104 to reflect the acceptance by the security guard of the visual check.

The microprocessor 104 would then check the site access database (not shown) to determine if additional biometric authorization is required for access to the site, by the person proffering the IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400. If the microprocessor 104 determines that additional biometric authorization is required for the person proffering the IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400, then the microprocessor 104 will display an "Obtain Thumbscan" message on the display 101, and the security guard will request a thumbscan from the person proffering the IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400.

The microprocessor 104 will perform a validation of the thumbscan read by the thumbprint scanner 210 and compare it with the biometric data read from the IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400 to determine if a sufficient match has been achieved to authorize access to the site. If the microprocessor 104 determines that the proffered thumbprint was not a sufficient match, then the microprocessor 104 will display a "Thumbscan Fail" message on the display 101 and the site access record database (not shown) is updated by the microprocessor 104 to reflect the failed thumbscan, and the security guard will take whatever action is appropriate for the circumstances.

If the microprocessor 104 determines that the proffered thumbprint was of a sufficient match by predetermined criteria then the microprocessor 104 will update the site access record database (not shown) to reflect the accepted thumbscan.

The microprocessor 104 will display an "Authorized" message on the display 101 and the site access record database (not shown) is updated by the microprocessor 104 to reflect that the person proffering the IC based 'dog-tag' 401 or a contactless IC based ID-card (Smart Card) 400 has been cleared for access to the site. The security guard will press a key on the keypad 102 to indicate to the program to acknowledge the authorized message, and the microprocessor 104 will update the site access record database (not shown) to reflect the acceptance of the authorization.

Whenever the handheld computer 100 recognizes that it has been placed within it's docking module (not shown), as is conventional, the microprocessor 104 will synchronize it's databases (not shown) with the site main database (not shown), to reflect any changes or accesses granted or denied since the last time it synchronized with the site database. At this time also any changes made to the site database are recorded in the database contained within the expansion module 200.

While the present invention has been described in connection with what is presently considered to be the most practical and preferred embodiments, it is to be understood that the invention is not to be limited to the disclosed embodiments, but to the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit of the invention, which are set forth in the appended claims, and which scope is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures.

CLAIMS

1. A handheld computer secure security identification terminal comprising:

a handheld computer including an expansion connector;

an expansion module including a mating connector;

the expansion connector connected to the mating connector; and

the expansion module including a microprocessor, a smart card proximity reader, an identification card reader, a thumbprint scanner and a multifunction secure access module.

2. The terminal of claim 1 further including a cryptographic validation routine complying with ISO Standard 15408.

3. The terminal of claim 1 further including a color display and a keypad electronically connected to each other via a bus.

4. The terminal of claim 1 in which the multifunction secure access module further includes a memory and encryption processor.

Figure 1.

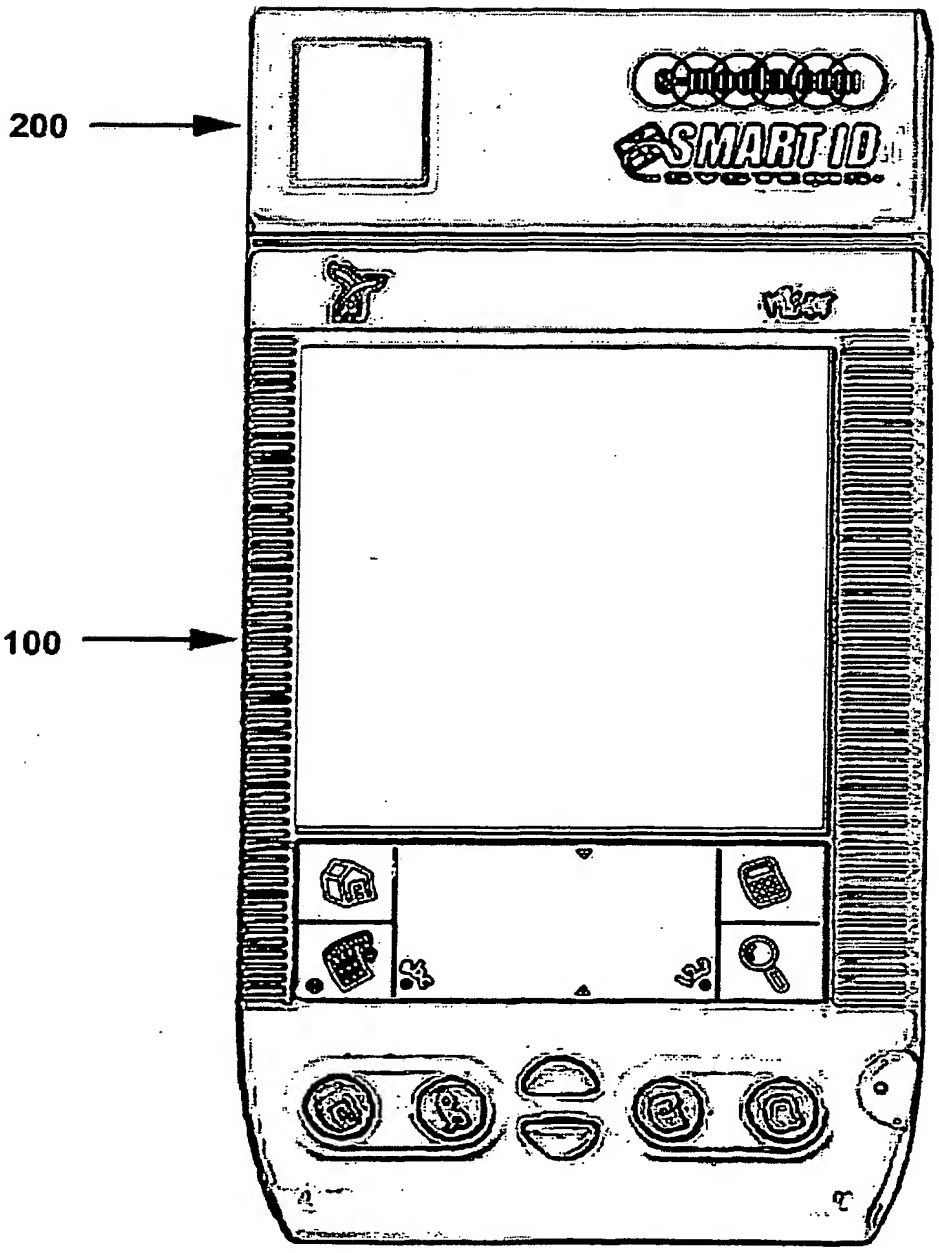


Figure 2.

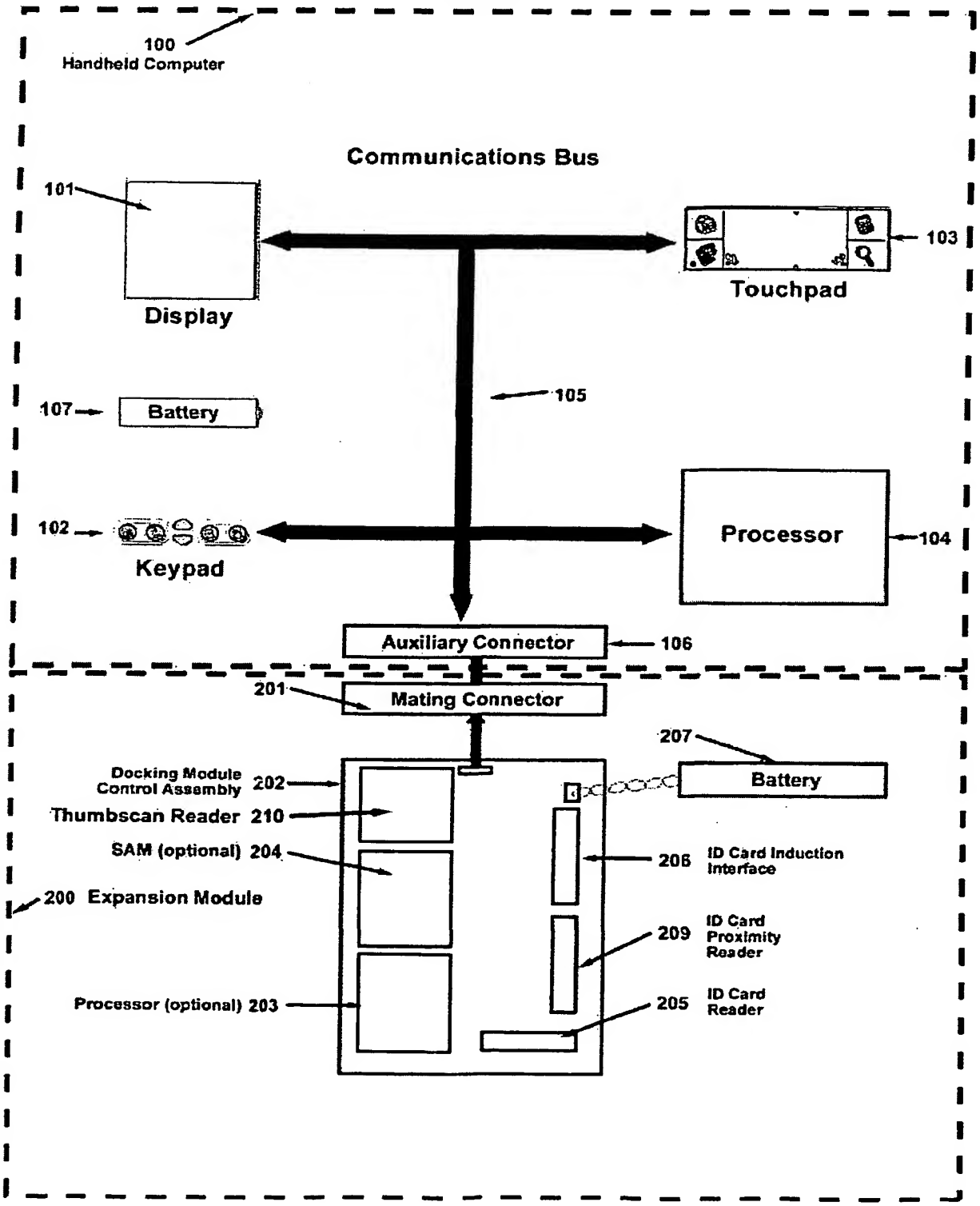

100
Handheld Computer
Communications Bus
101
Display
103
Touchpad
107
Battery
105
102
Keypad
Processor
104
Auxiliary Connector
106
201
Mating Connector
207
Battery
Docking Module Control Assembly 202
Thumbscan Reader 210
SAM (optional) 204
200 Expansion Module
Processor (optional) 203
206 ID Card Induction Interface
209 ID Card Proximity Reader
205 ID Card Reader

Figure 3.

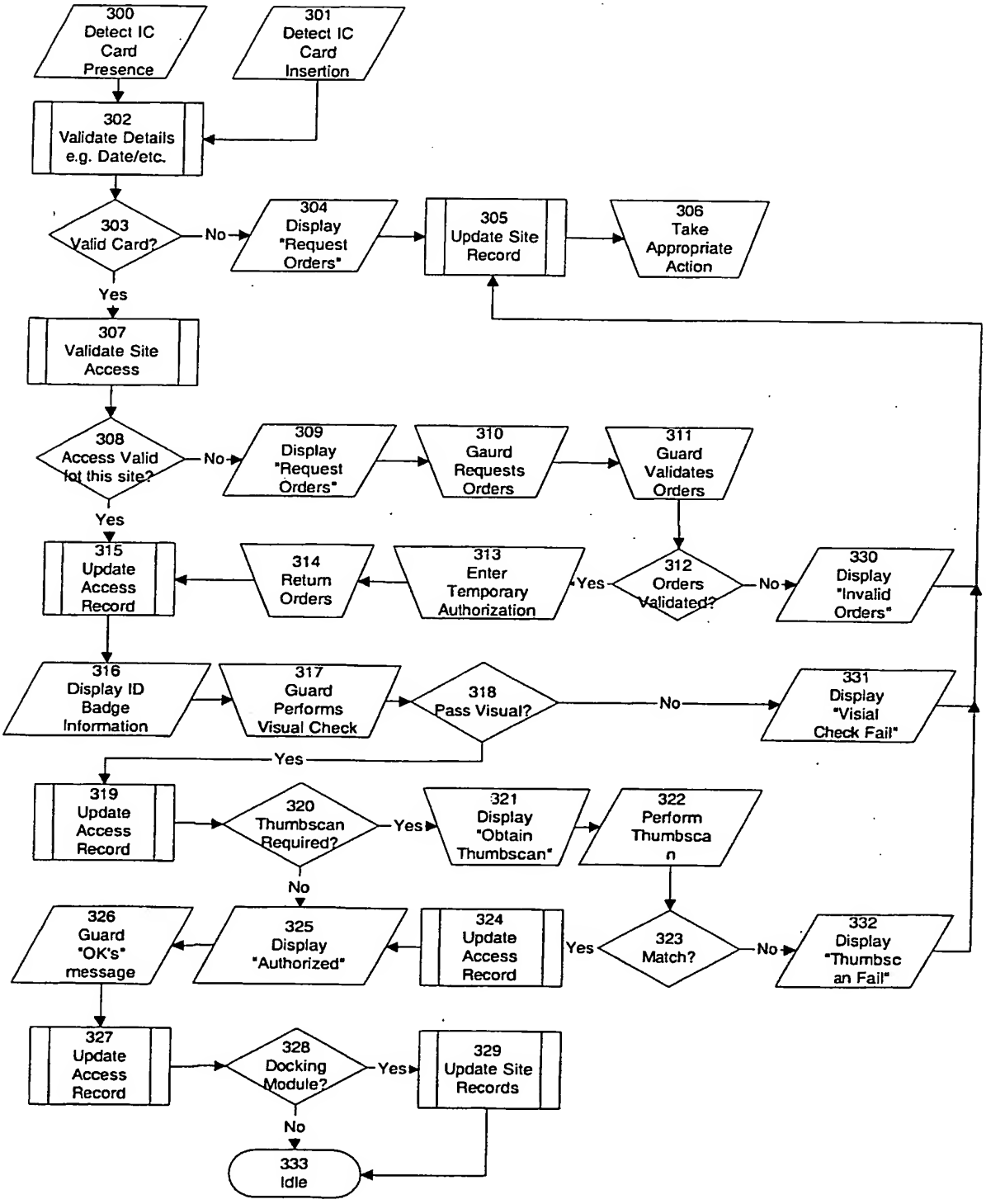


Figure 4.

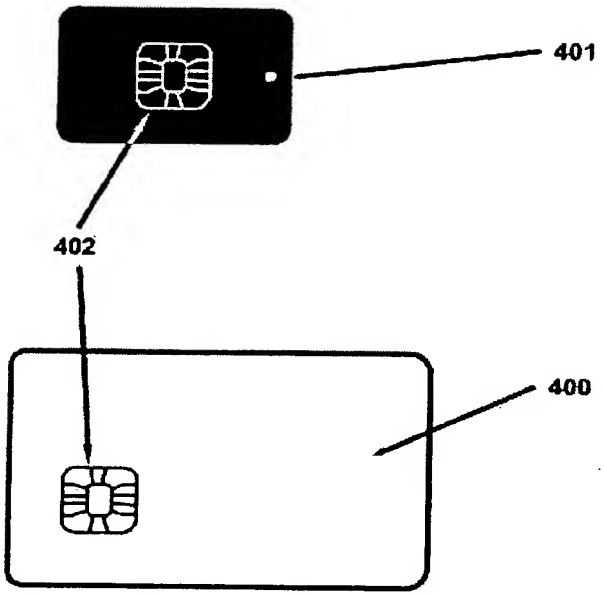


Figure 5.

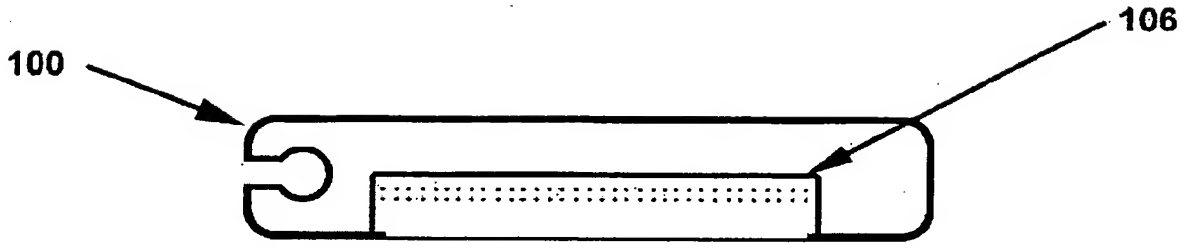


Figure 5b.

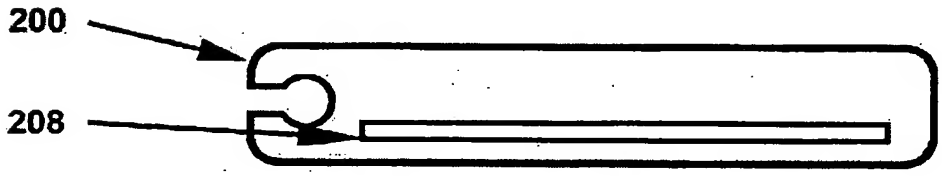


Figure 6.

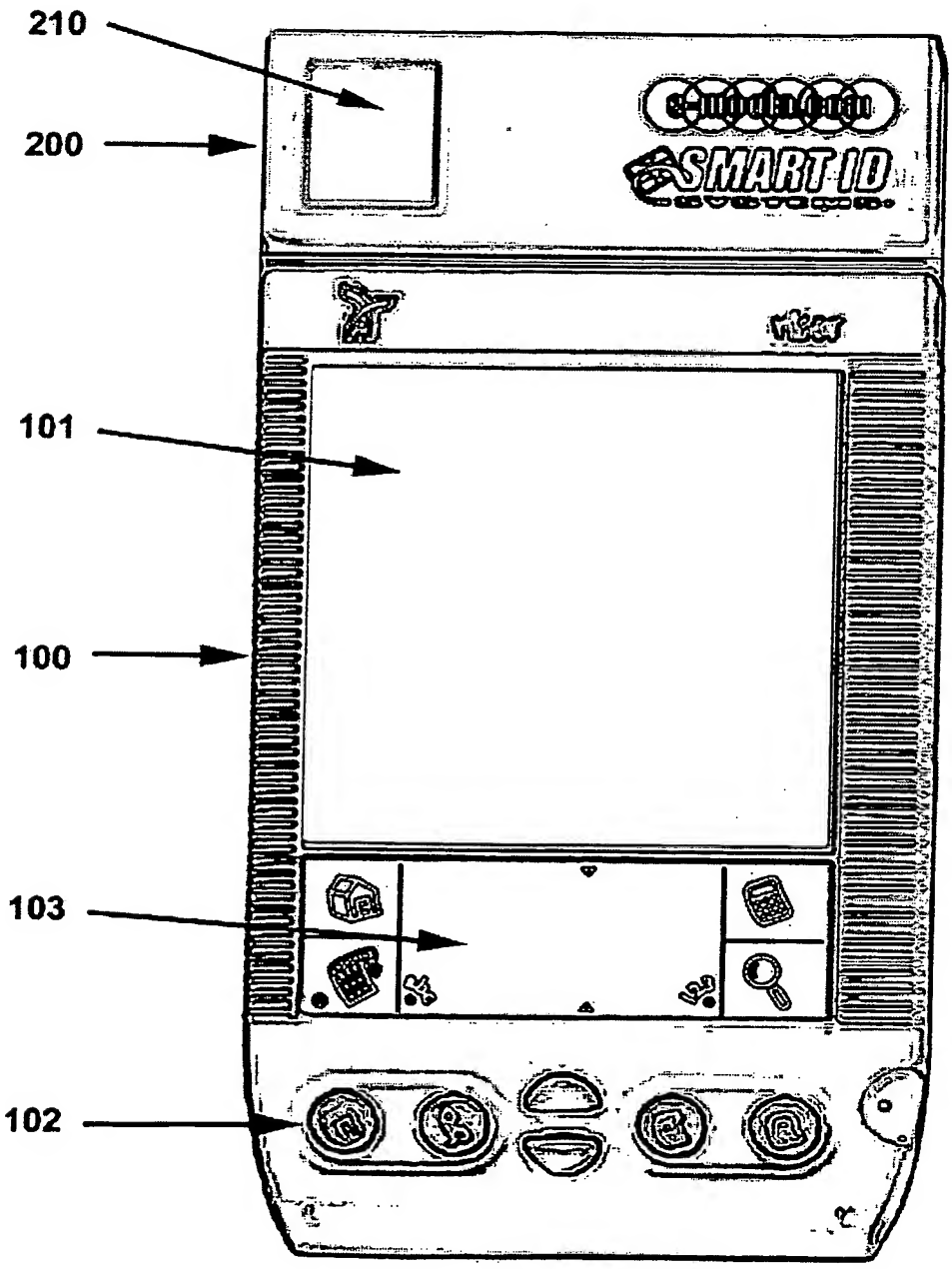


Figure 7.

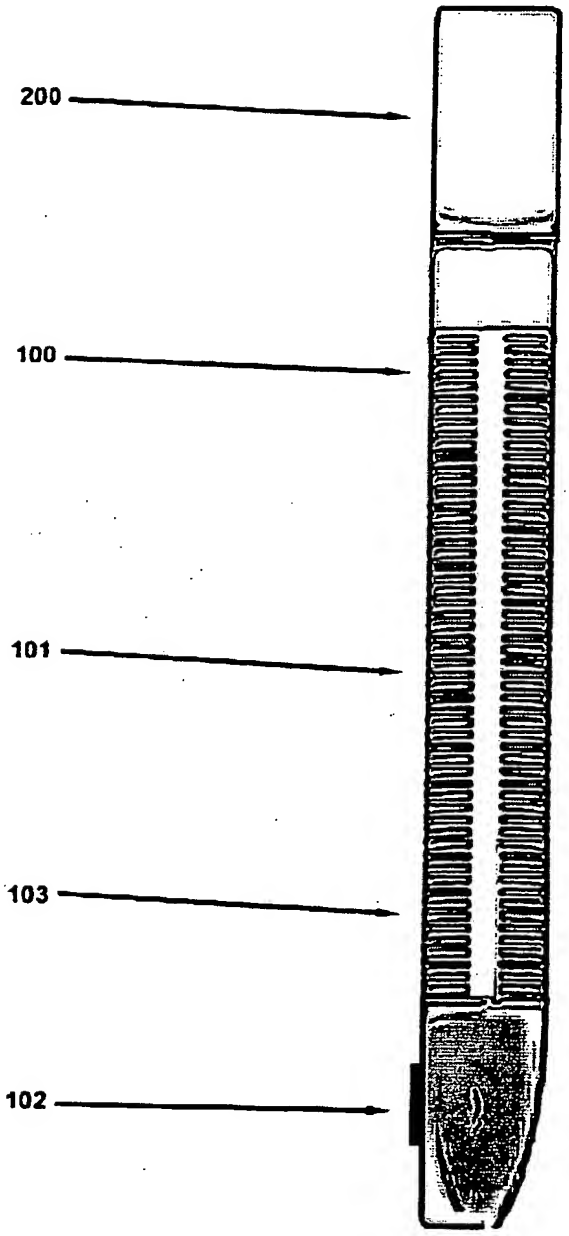
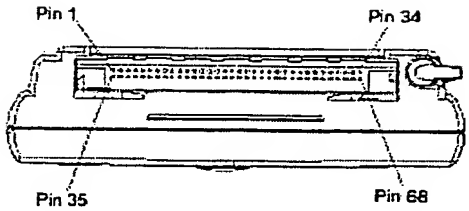


Figure 8.



Pin	Name	I/O/P/PU[1]	Function	Pin	Name	I/O/P/PU	Function
1	GND	P	Module Ground	35	GND	P	Module Ground
2	D3	I/O	Data Bus	36	CD1*	O/PU	Card Detect
3	D4	I/O	Data Bus	37	D11	I/O	Data Bus
4	D5	I/O	Data Bus	38	D12	I/O	Data Bus
5	D6	I/O	Data Bus	39	D13	I/O	Data Bus
6	D7	I/O	Data Bus	40	D14	I/O	Data Bus
7	CS0*[2]	I	Chip Select	41	D15	I/O	Data Bus
8	A10	I	Address Bus	42	CS1*	I	Chip Select
9	OE*	I	Output Enable	43	Reserved		Reserved
10	A11	I	Address Bus	44	Reserved		Reserved
11	A9	I	Address Bus	45	Reserved		Reserved
12	A8	I	Address Bus	46	A17	I	Address Bus
13	A13	I	Address Bus	47	A18	I	Address Bus
14	A14	I	Address Bus	48	A19	I	Address Bus
15	WE*	I	Write Enable	49	A20	I	Address Bus
16	IRQ*	O/PU	Interrupt Request	50	A21	I	Address Bus
17	VCC	P	Module VCC	51	VCC	P	Module VCC
18	VDOCK	P	Docking Voltage	52	VDOCK	P	Docking Voltage
19	A16	I	Address Bus	53	A22	I	Address Bus
20	A15	I	Address Bus	54	A23	I	Address Bus
21	A12	I	Address Bus	55	Reserved		Reserved
22	A7	I	Address Bus	56	Reserved		Reserved
23	A6	I	Address Bus	57	Reserved		Reserved
24	A5	I	Address Bus	58	RESET*	I	Module Reset
25	A4	I	Address Bus	59	Reserved		Reserved
26	A3	I	Address Bus	60	MIC-	I	Microphone
27	A2	I	Address Bus	61	MIC+	I	Microphone
28	A1	I	Address Bus	62	Reserved		Reserved
29	A0	I	Address Bus	63	LOWBAT*	I	Low Battery
30	D0	I/O	Data Bus	64	D8	I/O	Data Bus
31	D1	I/O	Data Bus	65	D9	I/O	Data Bus
32	D2	I/O	Data Bus	66	D10	I/O	Data Bus
33	Reserved		Reserved	67	CD2*	O/PU	Card Detect
34	GND	P	Module Ground	68	GND	P	Module Ground

1. I = input, O = output, and P = power, with respect to the module. For example, the IRQ signal is driven by the module and is an output to the handheld. PU indicates the signal is internally pulled up within the handheld.

2. * indicates an active low signal.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/06775

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 13/00
US CL : 710/300-304, 305-317
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 710/300-304, 305-317

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
N/A

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST, JPO, EPO, IBMTDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	US 6,222,726 B1 (CHA) 24 April 2001, col. 1 thru 6	1-4
X	Des. 429,170 (MAQUAIRE) 08 August 2000, Figures 1, 2	1-4
A	US 6,407,914 B1 (HELOT) 18 June 2002, Abstract; Figure 1; col. 1 thru col. 10	1-4

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
25 JUNE 2002

Date of mailing of the international search report
12 JUL 2002

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
RUPAL DHARIA
Peggy Harwood
Telephone No. (703) 305-4003

Form PCT/ISA/210 (second sheet) (July 1998)★